RM-11277

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the matter of	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket No. 96-115
Petition for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information	)	

PETITION OF
THE ELECTRONIC PRIVACY INFORMATION CENTER FOR RULEMAKING TO ENHANCE SECURITY AND AUTHENTICATION STANDARDS FOR ACCESS TO CUSTOMER PROPRIETARY NETWORK INFORMATION

Electronic Privacy Information Center
West Coast Office
944 Market Street, Suite 709
San Francisco, CA 94102

August 30, 2005

TABLE OF CONTENTS

SUMMARY

The Electronic Privacy Information Center ("EPIC") hereby petitions the Federal Communications Commission initiate a rulemaking proceeding to establish more stringent security standards for telecommunications carriers in releasing Consumer Proprietary Network Information ("CPNI"). CPNI is sensitive information collected by carriers that includes logs of calls that individuals initiate and receive on their phones. Section 222 of the Telecommunications Act makes clear that carriers have the duty of protecting CPNI, with particular emphasis on privacy concerns for personal, individualized data.[1] In implementing Section 222, the Commission has focused on the notice and disclosure requirements necessary to disseminate CPNI data to carrier affiliates and third parties for marketing purposes.[2] However, these efforts did not adequately address third party data brokers and private investigators that have been accessing CPNI without authorization. Data brokers and private investigators are taking advantage of inadequate security through pretexting, the practice of pretending to have authority to access protected records; through cracking consumers' online accounts with communications carriers; and possibly through dishonest insiders at carriers.[3] Prompt Commission action is necessary to insure that individualized CPNI is adequately protected from unauthorized third parties as required by Section 222.

In support, EPIC shows the following:

1. That online data brokers and private investigators widely advertise their ability to obtain CPNI without the account holder's knowledge and consent.

---

[1] 47 U.S.C. § 222 *et. seq.*

[2] *See, e.g.*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 F.C.C. Rcd 14860 (July 25, 2002).

[3] Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, Washington Post, Jul. 8, 2005, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070701862_pf.html.

2. That strong evidence exists showing the information was not acquired through legal channels. This evidence includes data brokers' advertising guarantees that they can obtain individuals' CPNI in a matter of hours, and that once obtained, the CPNI cannot be used in court.
3. That this unauthorized release of information suggests that the security and identification requirements carriers use to validate the identity of the CPNI requestor is insufficient to prevent unauthorized third parties from acquiring CPNI.
4. That the prevalence of this current practice and the possibility of further exploitation of lenient security standards create a significant privacy and security risk to carrier customers, one that must be addressed by prompt action by the FCC.

As a result of these concerns, the Commission should immediately initiate a rulemaking proceeding to (a) conduct an inquiry into the current method of security measures being used to verify the identities of those requesting individual CPNI, (b) to hear public comments in developing a security standard that would adequately address the privacy risks, and (c) establish a security standard by rule that heightens privacy of CPNI.

I. Section 222 of the Telecommunications Act requires that telecommunications carriers protect the privacy rights of customers by limiting access to CPNI

Congress enacted the Telecommunications Act of 1996, 47 U.S.C. § 222 *et. seq.*, in part to protect consumer privacy.[4] Section 222 of the Act obligates telecommunications carriers to protect the confidentiality of Consumer Proprietary Network Information ("CPNI").[5] Specifically, section 222(c)(1) states:

[4] *See* Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 F.C.C. Rcd 14860, 14862 (2002).
[5] 47 U.S.C. 222(c).

> Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.[6]

CPNI includes calling history and activity, billing records, and unlisted telephone numbers of service subscribers.[7] The Act therefore prohibits carriers from using, disclosing, or permitting access to CPNI without approval of the customer or as otherwise required by law if the use or disclosure is not in connection with the provided service, or listed as one of the exceptions provided for in Section 222(d).

In implementing Section 222, the Commission has focused on the notice and disclosure requirements necessary to disseminate CPNI data to carrier affiliates and third parties for marketing purposes.[8] Since the passage of the Telecommunications Act, the Commission has invited public comment and published orders regarding the extent to which carriers can provide aggregate CPNI to company affiliates and third parties, and what amount of customer notice and approval is necessary for providing this information.[9] However, the security standards necessary

---

[6] 47 U.S.C. § 222(c)(1).

[7] Section 222(f)(1) of the Telecommunications Act defines CPNI as follows:

> (A) Information that relates to the quantity, technical configuration, type, destination, and amount of use in a telecommunications service subscribed to by an customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of its carrier-customer relationship; and
>
> (B) Information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

[8] *See, e.g.*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 F.C.C. Rcd 14860, 14862 (2002).

[9] *Id.*

to protect against unauthorized solicitors pretending to be the customers themselves is an issue that deserves equal scrutiny, but has been inadequately addressed by the Commission thus far.

II. Congress accorded personal, individualized CPNI the greatest level of protection

The Telecommunications Act affects three categories of customer information to which different privacy protections and carrier obligations apply: (a) individually identifiable CPNI (b) aggregate customer information and (c) subscriber list information.[10] Congress afforded personal, individually identifiable information the greatest protection, and only allowed a carrier to disclose or permit access to such information, without customer approval, where necessary for providing telecommunications services, with four exceptions:

1. to initiate, render, bill and collect for telecommunications services
2. to protect the rights or property of the carrier, or to protect users and other carriers from fraudulent or illegal use of, or subscription to, such services
3. to provide inbound marketing, referral or administrative services to the customer for the duration of the call, if the call was initiated by the customer and the customer approves of the carrier's use to provide such service
4. To provide call location information concerning the user of a commercial mobile service in certain specified emergency situations.[11]

[10] *See* 47 U.S.C. 222(h) (providing specific definitions of each category of information).
[11] 47 U.S.C. § 222(d).

III. Unauthorized third parties are taking advantage of inadequate security and identity verification methods at the telecommunications carriers to access and sell individualized CPNI.

It is not disputed that carriers can provide individualized CPNI to the customer itself. In fact, every month, customers receive billing statements from carriers outlining their call history and rate charges. Many carriers now even have online account access, designed for customers to conveniently review their past or current account activity, billing information, addresses, etc. Carriers also have toll-free customer service numbers, which customers can call to request lost or misplaced statements and call records.

However, the security standards that carriers use to verify the identity of the CPNI requestor have been insufficient to prevent unauthorized third parties from acquiring and exploiting such data for personal and financial gain, providing a significant security loophole through which other privacy and security violations flow. Telecommunications carriers are not responsible for actively disseminating information to unauthorized third parties. Rather, unauthorized third parties have been exploiting security standards at the carriers to access and sell the information acquired through illegal means.

Online data brokers are firms that offer private investigation and other data services through Internet websites. These firms charge customers fees based on a graduated scale for the research services they provide, depending on the details of the data sought. Some offer to search for long-lost friends, relatives, or lovers. Others provide services specifically for spouses to spy on each other. Though some of the information these data brokers offer to retrieve and sell are available through public records, other information comes from proprietary sources, some of which is protected from disclosure by privacy statute or regulation.

For instance, some of these data brokers offer services to retrieve telephone call records. Some will retrieve it with only the telephone number provided, sometimes with turnaround times of 1-2 hours. For example, Intelligent e-Commerce, Inc. ("IEI"), a company that runs the online investigation website bestpeoplesearch.com, will provide detailed call records for the past 100 calls of either a business or residential phone line if the requestor provides the telephone number, name, and address of the account holder. (Attachment A and B are complaints to the Federal Trade Commission concerning this company.) Though IEI specifies 1 to 5 days as necessary to retrieve the records, another data broker, Infonowusa.com offers a 1 to 3 hour turnaround time for detailed cell phone call records. (Attachment C is a list of an additional 40 web sites offering to sell CPNI to third parties.)

These telephone call records are protected as CPNI under the Telecommunications Act, and particularly protected as individually identifiable CPNI (as opposed to aggregate customer information or subscriber list information). These online private investigators do not reveal how they actually obtain this information. However, EPIC is aware of no legal way to reliably and quickly obtain call detail information. Nor does it appear possible for them to reliably obtain this information within the time frames they claim without making misrepresentations (pretexting) to telecommunications carriers or soliciting the carriers to violate the Telecommunications Act.

Additionally, two professional licensed investigators were quoted agreeing with EPIC's assessment in recent media reports:

> [Francie] Koehler, who was part of a project to research online private investigations services, said, "I know that many of them claim to get the information legally. I don't understand how that happens." When she's tried to get someone's phone records via

subpoena, she said, "Every time you try, they send the telephone company lawyer in to quash the subpoena."[12]

Washington Post journalist Jonathan Krim quoted Robert Townsend, an advocate of investigator licensure and best practices:

> "I do not know of any legal way to obtain a person's telephonic history," Robert Townsend, head of the National Association of Legal Investigators, said in an interview. Townsend added that he thinks only a small minority of licensed investigators engage in the practice of acquiring and selling the data.[13]

In addition to providing suspiciously fast "turn around times," many also represent that the information provided is "confidential" and not admissible in courts. In some cases, the sites specify that the client must employ a legal method, such as a subpoena, for obtaining the same data if the client wants to use the information in court. These practices suggest that no official process is being employed to obtain the records legally.

It also appears that these violations are occurring at an alarming rate. The cost building the infrastructure to offer call record data is substantial, yet many companies offer to sell this data. These companies must maintain a website, have contacts with investigators in many states, and process transactions quickly (some as quickly as 1-2 hours). There is a risk that there will be no "hit," resulting in the online data broker performing services without compensation. Many sites offer this service through "sponsored links" on popular search engines and other forms of online advertising, further adding to the cost of offering the data. Combined, these factors and

---

[12] Susan Kuchinskas, *EPIC Fighting Online Phone Record Sales*, InternetNews, July 8, 2005, available at http://www.internetnews.com/ent-news/article.php/3518851.

[13] Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, Washington Post, Jul. 8, 2005, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070701862_pf.html.

the large number of entities offering call records online suggests that many individuals' phone records are being illegally access and sold every day to simply cover the cost of doing business.

Telecommunications carriers are the primary source of CPNI; therefore, they should be the first line of defense against these practices of illegitimately accessing and selling CPNI. Through Section 222, Congress specifically placed the burden of protecting CPNI in their hands.[14] The Commission has recognized the importance of CPNI security, particularly with regards to the requirements for customer notification in releasing such information to allowed parties under Section 222. It is therefore alarming that these online data brokers are gaining access to these call records without the customers' consent or even knowledge. Regardless of how illegitimate the practices of the online data brokers may be, they would not be possible were it not for loopholes in the security measures that telecommunications carriers use to verify the identity of the CPNI requestor. Carriers may be contributing to this practice by only requiring a few pieces of easily-obtained biographical information (such as date of birth, mothers maiden name, or the Social Security number) to change the addresses on the phone records or requesting call history data. This type of biographical information can be easily obtained by a third party through public records and used to gain access to CPNI. Many different websites have millions of records on date of birth. And online data brokers often have access to other databases to purchase Social Security numbers or dossiers that would contain the mother's maiden name.

IV. The prevalence of this practice poses a significant privacy and security risk for telecommunications customers.

Individuals are likely to suffer injury as a result of these ongoing practices of selling CPNI. The release of such information without a customer's knowledge can lead to devastating

[14] *See* 47 U.S.C. § 222(c)(1).

results and create serious consequences in the area of personal privacy. With the advent of cellular phones, call records contain some of the most sensitive and private information an individual may have. Phone records can be used to track an individual's daily habits, to spy on a person's communications with others, or to stalk another person. We are also aware of data brokers who offer location tracking services for wireless phone users, even though this information, under Section 222(d), is only supposed to be used for authorized emergency purposes (See services of CSI, Attachment C).[15] Furthermore, if online data brokers are acquiring their information by accessing customers' online accounts, they might also have access to the individual's billing address, credit card information, and even their social security number. These pieces of personal information are so often used in security verification for other services that possessing this information would put the online data broker in complete control of the individual's electronic identity.

Individual phone records are not the only ones at risk. Some websites claim to be able to access any phone record with only a phone number, name, and address. Some even boast the ability to provide business telephone records (See Attachment C). Given the prevalence of phones, both wired and wireless, used for business purposes, these services could be (and most likely are being) used for industrial espionage and other illicit business activities. Business phone records yield sensitive information about client lists and contact information, resulting in privacy violations both for the businesses and the people that those businesses have contacted.

---

[15] Section 222(d)(4) of the Telecommunications Act provides that the location of a cellular phone should only be revealed in the following instances:

> (A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;
> (B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or
> (C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

While the Commission has tried to balance competition, access, and privacy rights in determining the best method with which to enforce Section 222, the types of privacy violations described here are unauthorized, unwarranted, and serve more to promote security breaches and industrial sabotage than competition.

Furthermore, these business are operating online, and provide these data brokerage services readily at the submission of an Internet form and upon receipt of payment. They do not actually meet their clients and assess the clients' intent in trying to access these records. They have no way of screening out clients who desire access to such phone records for malicious purposes. Therefore, weak security standards may also pose as a security threat to the very customers whose privacy the Commission is striving to protect.

V. The Federal Communications Commission should immediately initiate a rulemaking proceeding to address the CPNI protection measures used by telecommunications carriers and invite comment to develop adequate safeguards for verifying the identity of parties trying to access CPNI.

Given the privacy and security issues at stake in this matter, the Commission should immediately initiate a rulemaking proceeding to investigate the following issues:

1. What security measures telecommunications carriers currently have in place for verifying the identity of people requesting CPNI.
2. What inadequacies currently exist in those measures that allow third parties outside of the realm of Section 222, such as online data brokers and private investigators, to access individual CPNI without the customer's knowledge or authorization.
3. What kind of security measures are warranted to better protect telecommunications customers from unauthorized access to personal and individualized CPNI.

Some forms of security measures that would more adequately protect access to CPNI might include the following:

1. Consumer-set passwords. Currently, there is a reliance on biographic identifiers, such as the Social Security Number and date of birth, to authenticate individuals. These biographic identifiers are inadequate for authentication, because, unlike passwords, they do not change, and they are widely available. A unique and separate password chosen by the account holder at the time of phone activation would greatly increase security of CPNI.
2. Audit trails. Carriers should be under a duty to record all instances where a customer's record is accessed, whether there has been a disclosure of information, and to whom the information has been disclosed. Audit trails deter insiders from selling personal information, and once data is accessed without authorization, audit trails aid in investigating the security breach.
3. Encryption. When stored at the carrier, data should be encrypted. While audit trails help protect against insider abuse, encryption assists in protecting data from security threats outside the corporation.
4. Notice to affected individuals and the Commission when there is a security breach. In many other sectors, companies must notify individuals if a security breach results in their personal information being accessed by an unauthorized person. This allows individuals to mitigate harm from the breach, and assists in the public in understanding whether data are actually secure.
5. Limiting Data retention. Call detail records should be deleted after they are no longer needed for billing or dispute purposes. Alternatively, carriers should be required to

deidentify records, that is, divorce identification data from the transactional records. This will allow carriers to maintain call records for data analysis, but reduce the risk that the same records will be associated with an account holder and used to invade privacy.

Respectfully Submitted,

Chris Jay Hoofnagle
Senior Counsel
August 30, 2005

Before the
Federal Trade Commission
Washington, DC

In the Matter of	)
	)
Intelligent e-Commerce, Inc.	)
	)

Complaint and Request for Injunction, Investigation and for Other Relief

INTRODUCTION

1. This complaint concerns the sale of consumer information by Intelligent e-Commerce, Inc. ("IEI"). As set forth in detail below, IEI is engaged in unfair or deceptive acts or practices as defined by Section 5(a) of the FTC Act. Moreover, IEI is violating or causing violations of the Telecommunications Act of 1996 ("Telecommunications Act") and 39 CFR § 265.6 ("Postal Regulations").

2. IEI is an e-Commerce consulting service that operates bestpeoplesearch.com, an Internet investigative service. IEI advertises and provides online ordering forms for its customers to obtain a variety of information about consumers in the U.S. and Canada.[1] Such information includes detailed phone call records as well as the addresses on file for post office box and private mailbox holders. These categories of personal information are protected by regulation or statute, and cannot be obtained without legal justification, but are nevertheless offered for sale on bestpeoplesearch.com. We urge the Federal Trade Commission to take immediate action to investigate IEI's information brokerage activities and to enjoin IEI from selling information collected in violation of federal law.

3. Bestpeoplesearch.com is one of many investigation "portal" sites that offer for sale personal information that is protected by statutes. Like bestpeoplesearch.com, these other sites contain language suggesting that the information is obtained by illegitimate means (investigators rely upon "confidential sources" and information provided is "confidential" and not "admissible in court"). These sites demonstrate a pattern of questionable personal information sales online. We therefore urge the Commission to initiate an industry-wide investigation into online investigation sites.

[1] *See e.g.* Bestpeoplesearch.com, *Ontario, Canada Residential Long Distance Phone Records*, available at https://secure.bestpeoplesearch.com/ontario-canada-residential-long-distance-phone-records/c-RDPB,s-CAON,Service.aspx (last visited June 15, 2005) (offering for sale long distance calling records of individuals in Ontario). A complete archive of the bestpeoplesearch.com website is attached to this complaint as bestpeoplesearch.zip.

PARTIES

4. The Electronic Privacy Information Center ("EPIC") is a non-profit research organization based in Washington, D.C. EPIC's activities include the review of government and private sector polices and practices to determine their possible impact on the privacy interests of the American public. Among its other activities, EPIC has prepared reports and presented testimony before Congress and administrative agencies on the Internet and privacy issues. EPIC opposes unscrupulous practices in the information brokerage industry, and recently filed an amicus brief[2] in *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001 (N.H., 2003), a case in which the New Hampshire Supreme Court held that an information broker is potentially liable for the harms caused by selling personal information.

5. IEI is an e-Commerce consulting service based in Encinitas, California. (Exhibit A.) IEI maintains bestpeoplesearch.com, a portal for obtaining personal information. (Exhibit B.)

THE IMPORTANCE OF PRIVACY PROTECTION

6. The right of privacy is a fundamental right in the United States. The privacy of an individual is directly implicated by the collection, use, and dissemination of personal information. Disclosure of private information to third parties is protected through a number of statutes and regulations, including certain provisions of the Telecommunications Act and Postal Regulations. One purpose of these statutes is to protect consumers from the harms that can arise from others obtaining their private information for improper purposes. The release of such information without a consumer's knowledge can lead to devastating results, including identity theft and fraud.

7. Individuals are likely to suffer injury as a result of IEI's ongoing practice of selling personal information. The Drivers Privacy Protection Act, which protects personal information in motor vehicle records, was passed in reaction to the 1989 death of actress Rebecca Schaeffer.[3] A private investigator, hired by an obsessed fan, was able to obtain her address through California motor vehicle records.[4] The fan used her address information to stalk and to kill her.[5] The Postal Regulations were adopted in response to similar concerns, in particular concerns raised by advocates for battered women who otherwise could not safely receive mail.[6]

8. The potential harm caused by unscrupulous information brokerages is further addressed in *Remsburg v. Docusearch, Inc.*, in which the New Hampshire Supreme Court held that information brokers and private investigators could be liable for the harms caused by selling personal information.[7] In that case, a stalker obtained a young woman's personal information, including her Social Security number and employment information, from an internet-based

---

[2] Brief of Amicus Curiae Electronic Privacy Information Center, *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, (N.H. 2003), *available at* http://www.epic.org/privacy/boyer/brief.html.
[3] Brad Bonhall, *Modem Operandi*, Los Angeles Times, April 24, 1994, at E1.
[4] Aurora Mackey Armstrong, *Private Eyes, Private Lives*, Los Angeles Times, July 19, 1990. at J10.
[5] *Id.*
[6] James Bovard, *Postal Service Bites Private Mailbox Users*, USA Today, July 8, 1999, at A13.
[7] *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001 (N.H. 2003).

private investigation, pretexting, and information service, and then used this information to locate and murder the woman.

9. IEI is aware of the potential harm that can result from providing this information, as it attempts to disclaim a wide variety of harms in its Terms and Conditions ("Terms"). The Terms require that the requestor take the following pledge: "I also do hereby faithfully pledge, that my desire to locate the data or individual described above in no way involves any intention on my part to harm, to cause harm, to harass, to stalk (as described by applicable laws), or to otherwise take any illegal or proscribed action against any person or entity." (Exhibit C.) IEI also requires information requestors to indemnify the company from harms flowing from the use of personal data. (Exhibit C.)

BASIS FOR ACTION

10. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), renders unfair or deceptive acts or practices in or affecting commerce unlawful. Misrepresentations of material facts constitute deceptive acts or practices and are unlawful pursuant to Section 5(a) of the FTC Act. Under Section 5(n) of the FTC Act, an act or practice is unfair if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and that is not outweighed by countervailing benefits to consumers or to competition.[8]

11. Several categories of information offered for sale by IEI are not available except by misrepresentation or fraud in the violation of a federal statute. These misrepresentations are similar to the misrepresentations made by the defendant information brokers in *FTC v. Information Search, Inc.*,[9] as well as the misrepresentations in numerous cross-border lottery ticket sales cases pursued by the FTC, e.g. *FTC v. World Media Brokers, Inc.*[10]

12. Although IEI claims to use private investigators to obtain this information, in no way does this make its actions legal or constitute any significant barrier to harm. Private investigators are regulated by a wide range of state laws, with licensing requirements ranging from simple payment of a licensing fee[11] to extensive occupational training and experience.[12] None of these schemes, however, give private investigators special rights to solicit others to violate the law.

13. By obtaining and selling private information about consumers that is not legally available, or is only available for narrowly-defined purposes, IEI has almost certainly caused substantial injury to consumers, and is likely to cause additional injury. Because its entire business consists of surreptitiously obtaining information about consumers, this injury is not avoidable at all by the consumers themselves. The service of unlawfully obtaining and reselling information about consumers does not provide countervailing benefits to consumers or to competition.

---

[8] 15 U.S.C. § 45(n).
[9] Stipulated Final Judgment, *FTC v. Information Search, Inc.* (No. AMD01-1121), *available at* http://www.ftc.gov/os/2002/03/infosearchstip.pdf.
[10] Complaint, *FTC v. World Media Brokers Inc.* (No. O2C-6985), *available at* http://www.ftc.gov/os/2002/12/emscmp.pdf.
[11] Ala. Code § 40-12-93.
[12] Cal. Bus. & Prof. Code § 7541.

SPECIFIC PRACTICES

Obtaining and Selling Information in Violation of the Telecommunications Act

14. Congress enacted the Telecommunications Act of 1996, 47 U.S.C. § 222 *et. seq.*, to stimulate competition in telecommunication services, while protecting the privacy of the consumer. Section 222 of the Act provides that telecommunications carriers must protect the confidentiality of Consumer Proprietary Network Information ("CPNI"). CPNI includes calling history and activity, billing records, and unlisted telephone numbers of service subscribers.[13] The Act prohibits carriers from using CPNI even for their own marketing purposes. Furthermore, the Act prohibits carriers from using, disclosing, or permitting access to CPNI without approval of the customer or as otherwise required by law if the use or disclosure is not in connection with the provided service.[14]

15. IEI has misrepresented its right to legally obtain, or cause others to obtain, this protected information. It offers for $187, "Cell Phone Package - includes Name, Address and Call Records" for customers who wish to purchase a copy of a third party's cellular phone record. (Exhibit D.) IEI represents that, "Cell Toll Reports are obtained by private investigators for your personal informational purpose only. These reports are NOT valid in a court of law." (Exhibit D.) This representation suggests that the records were obtained in an illegitimate, illegal, or unverifiable fashion, thus jeopardizing their admissibility in a legal action.

16. IEI also advertises the sale of protected residential telecommunication activity. It offers, for $87, the "Residential Local/LATA Phone Records" for customers who wish to purchase a copy of a third party's residential long distance bill for the last billing cycle. (Exhibit E.) IEI represents that, "This search is for RESEARCH purposes ONLY. If you find information contained in our reports and need them for legal purposes you must subpoena the records from the telephone carrier to use them in a court of law. This is a confidential report between Best People Search and you (our client)." (Exhibit E.) Again, this representation suggests that the records were obtained in an illegitimate, illegal, or unverifiable fashion, thus jeopardizing their admissibility in a legal action.

17. IEI does not represent how private investigators actually obtain this information, but it does not appear possible for them to reliably obtain this information without making misrepresentations (pretexting) to telecommunications carriers or soliciting the carriers to violate the Telecommunications Act.

Obtaining and Selling Information in Violation of 39 CFR § 265.6

18. The federal regulations governing release of information about owners of private mailboxes and post office boxes tightly regulate the release of this information, which may only be provided: (1) to a federal, state or local government agency upon prior written certification that the information is required for the performance of its duties, (2) to a person who certifies, in

[13] 47 U.S.C. §222(h)(1)
[14] 47 U.S.C. §222(c)

detail, that the information is necessary to serve process in an ongoing lawsuit, (3) in response to a subpoena or court order. In the event that the box owner files with the postmaster a protective court order, the information may only be provided in response to a court order.[15]

19. IEI has misrepresented its right to legally obtain, or cause others to obtain, this information. It offers, for $77, "PO Box Search (Reverse P.O. Box Lookup)." (Exhibit F.) IEI claims that this information is obtained by working with a Postal Inspector: "Investigators work with postmasters all over the USA. It is up to the individual Postmaster whether they want work with the investigator..." (Exhibit F.) This representation suggests that the method of obtaining the information is illegitimate. If a legal, legitimate course of action can yield these records, whether a Postmaster was willing to "work" with investigators would be irrelevant.

20. IEI also offers, for $97, "Reverse Private Mail Box Lookup." (Exhibit G.) Again, IEI represents that investigators "work" with companies to obtain this information: "Investigators work with personal mail box companies to obtain your requested information. It is up to the individual mail box retail center whether they want work with the investigator." (Exhibit I.) It does not appear possible for investigators to reliably obtain this information without making misrepresentations to PMB business owners or soliciting them to violate 39 CFR § 265.6.

OTHER SITES PROVIDING ONLINE INVESTIGATION SERVICES

21. A search in the Google search engine returns many sites, both as sponsored links, and as normal search results, of online investigator sites similar to bestpeoplesearch.com. Many of these sites offer sales to the general public.

22. Abika.com offers call detail[16] and the actual identity of people who use screen names on AOL, Match.com, Kiss.com, Lavalife, and Friendfinder.com.[17]

23. Peoplesearchamerica.com offers call detail[18] and P.O. Box records.[19]

24. Onlinepi.com offers cell phone location information.[20]

25. Discreetresearch.com offers call detail.[21]

26. Datatraceusa.com offers call detail.[22]

---

[15] 39 CFR 265.6(d)(4) and (d)(8).
[16] *See* http://www.abika.com/Reports/TracePhoneCalls.htm (last visited June 22, 2005).
[17] *See* http://www.abika.com/Reports/tracepeople.htm#Search%20Address/Phone%20Number%20associated%20with%20email%20Address%20or%20Instant%20Messenger%20Name. (last visited June 22, 2005).
[18] *See* http://www.peoplesearchamerica.com/Cell%20Tolls.htm (last visited June 22, 2005).
[19] *See* http://www.peoplesearchamerica.com/Address-Search.htm (last visited June 22, 2005).
[20] *See* http://www.onlinepi.com/searches/PS/ps15.htm (last visited June 22, 2005).
[21] *See* http://www.discreetresearch.com/restolls.htm (last visited June 22, 2005).
[22] *See* http://www.datatraceusa.com/products.asp (last visited June 22, 2005).

REQUEST FOR RELIEF

Wherefore, the Complainants request that the Commission:

A. Initiate an investigation into the information collection practices of IEI;

B. Order IEI to immediately stop the advertisement for sale of legally protected personal information on their website bestpeoplesearch.com and any other of their similar websites;

C. Order IEI to fully comply with the Telecommunications Act regulations and 39 CFR § 265.6;

D. Order IEI to destroy all records collected for customers about third parties which they have obtained through illegal means;

E. Seek legislation giving consumers protections against pretexting outside the financial services sector.

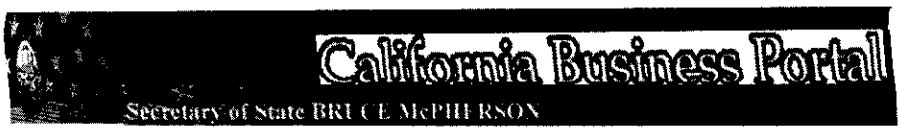
F. Provide such other relief as the Commission finds necessary to redress injury to consumers and third parties resulting from IEI's practices as described herein.

G. Conduct additional investigations into the many other web-based businesses offering similar services.

Respectfully Submitted,

Chris Jay Hoofnagle
Senior Counsel
ELECTRONIC PRIVACY INFORMATION CENTER
WEST COAST OFFICE
944 Market St. #709
San Francisco, CA 94102
(415) 981-6400

Submitted July 7, 2005



DISCLAIMER: The information displayed here is current as of JUN 10, 2005 and is updated weekly. It is not a complete or certified record of the Corporation.

Corporation

INTELLIGENT E-COMMERCE, INC.

Number: C2292987 **Date Filed:** 12/19/2002 **Status:** active

Jurisdiction: California

Address

119 N EL CAMINO REAL STE 136

ENCINITAS, CA 92024

Agent for Service of Process

NOAH WIEDER

119 N EL CAMINO REAL STE 136

ENCINITAS, CA 92024

For information about certification of corporate records or for additional corporate information, please refer to Corporate Records. If you are unable to locate a corporate record, you may submit a request to this office for a more extensive search. Fees and instructions for requesting this search are included on the Corporate Records Order Form.

Blank fields indicate the information is not contained in the computer file.

If the status of the corporation is "Surrender", the agent for service of process is automatically revoked. Please refer to California Corporations Code Section 2114 for information relating to service upon corporations that have surrendered.

directNIC

Home Search Sign-Up My Account Help Shopping Cart

June 15, 2005

About This Page:

A whois search allows you to find the registered owner of a domain name in the central Shared Registry System.

Need Help?

- FAQ
- Trouble Ticket System
- Resource Center
- User Guides

Search the WHOIS Database

bestpeoplesearch.com WHOIS

Include the TLD (i.e. .com, .uk, etc.)

Related Domains

bestpeoplesearch.ws	Available	Click here to add to cart!
bestpeoplesearch.net	Available	Click here to add to cart!
bestpeoplesearch.biz	Available	Click here to add to cart!
bestpeoplesearch.us	Available	Click here to add to cart!
bestpeoplesearch.org	Available	Click here to add to cart!
bestpeoplesearch.com.cn	Available	Click here to add to cart!
bestpeoplesearch.net.cn	Available	Click here to add to cart!
bestpeoplesearch.org.cn	Available	Click here to add to cart!
bestpeoplesearch.cn	Available	Click here to add to cart!
bestpeoplesearch.name	Available	Click here to add to cart!

Whois Search Results

The data contained in the WHOIS database, while believed by the company to be reliable, is provided "as is", with no guarantee or warranties regarding its accuracy. This information is provided for the sole purpose of assisting you in obtaining information about domain name registration records. Any use of this data for any other purpose, including but not limited to, allowing or making possible dissemination or collection of this data in part or in its entirety for any purpose, such as the transmission of unsolicited advertising and solicitations, is expressly forbidden without the prior written permission of this company. You may not use the data to *allow, enable, or otherwise support any marketing activities*, regardless of the medium used. Such media include but are not limited to e-mail, telephone, facsimile, postal mail, SMS, and wireless alerts. In addition, you may not sell or redistribute the data. By submitting an inquiry, you agree to these terms of usage and limitations of warranty. Please limit your queries to 10 per minute and one connection.

Domain Services Provided By:
NamesDirect.com, support@namesdirect.com
http://www.transferyourdomain.com/

Registrant:
Intelligent e-Commerce, Inc.
intelligent ecommerce
San Diego, CA 92039
US

Registrar: NAMESDIRECT
Domain Name: BESTPEOPLESEARCH.COM
Created on: 02-NOV-02
Expires on: 11-JUL-06
Last Updated on: 12-JUN-04

Administrative, Technical Contact:

helpREMOVENOSPAM@intelligentecommerce.com
Intelligent e-Commerce, Inc.
PO Box
La Jolla, CA 92039
US
858-777-3326

Domain servers in listed order:

dns2.siteplot.com
ns0.siteplot.com

End of Whois Information

Search the WHOIS Database

bestpeoplesearch.com WHOIS
Include the TLD (i.e. .com, .uk, etc.)

About *direct*NIC | Legal Information | Site Map

Contact BestPeopleSearch.com

Address:
Intelligent e-Commerce, Inc.
c/o BestPeopleSearch.com
119 N. El Camino Real #136
Encinitas, CA 92024

Customer Support Email: support@bestpeoplesearch.com

Phone: 760-652-4050
Fax: 858-777-3326

Questions?
E-mail: support@bestpeoplesearch.com

Terms and Conditions

Terms & Conditions:

BestPeopleSearch.com Agreement

This agreement sets forth the terms and conditions under which the website known as BestPeopleSearch.com may be used. Please read all the information contained in this agreement. Use of this service is expressly contingent upon agreement to the terms and conditions set forth herein.

DEFINITIONS:

Customer: You, your affiliate, subsidiaries, dba's, shareholders, directors, predecessors, successors, assigns agents, attorneys, employees, and representatives of every nature.

IEI: Intelligent e-Commerce, Inc., BestPeopleSearch.com and or any of its affiliates, subsidiaries, dba's, shareholders, directors, predecessors, successors, assigns, agents, attorneys, employees, and representatives of every nature.

Third Parties: A person or entity that is not a party to this contract, but has an involvement (such as, but not limited to, one who is a buyer from or seller to one of the parties to this agreement, otherwise provides services or is the subject of or a relation to any subject(s) of any information request).

Data: For the purpose of this agreement, data is defined as any address, phone number, DMV information, and/or Social Security Number information provided to me by IEI, which will allow me direct or indirect (through a third party) contact with the party sought if so intended. IEI cannot and does not make any guarantee as to the results of any search. IEI can only conduct its search based upon the information and criteria provided by me.

GENERALLY

Upon submission of my search request to BestPeopleSearch.com, I ("Customer") understand, acknowledge and agree that I have retained the services of Intelligent e-Commerce, Inc. (hereinafter "**IEI**") for the purpose of researching my request for the applicable fee. I understand that IEI is merely a conduit between those desiring information and those who provide it. I understand that IEI will not review the information that I provide for accuracy or for any other reason. Customer understands and agrees that the fee paid to IEI by customer is paid by Customer for the time and labor expended by Third Parties in researching and locating the information and not for the information itself.

NO LIABILITY FOR ACTS OR OMISSIONS OF THIRD PARTIES

I understand that IEI does not provide the investigation services required to provide the information requested by me and only passes the exact information provided to third party investigation services who then conduct whatever research they deem appropriate in their sole discretion. Customer acknowledges and agrees that IEI has no control over how or by what means the information provided was acquired and customer expressly releases, indemnifies and agreed to hold harmless and defend IEI. Customer agrees that he/she shall not seek to hold IEI liable under any circumstances for information sought, information provided or methods used to acquire it.

CONFIDENTIALITY OF DATA

Although **IEI** will use all reasonable efforts to safeguard the confidentiality of your Data, transmissions made by means of the Internet cannot be made absolutely secure and I understand and accept this as potential outcome. **IEI** will have no liability for disclosure of Data for any reason including but not limited to errors in transmission or unauthorized acts of third parties.

DISCLAIMER AND LIMITS

The information from or through the site is provided "as available," and all warranties, express or implied, are disclaimed (including but not limited to the disclaimer of any implied warranties of merchantability and fitness for a particular purpose). The information and services may contain bugs, errors, problems, inaccuracies or other limitations. IEI, and its affiliated parties, have no liability whatsoever for your use of any information or service. In particular, but not as a limitation thereof, IEI and its affiliated parties are not liable for any indirect, special, incidental or consequential damages (including damages for loss of business, loss of profits, litigation, or the like), whether based on breach of contract, breach of warranty, tort (including negligence), product liability or otherwise, even if advised of the possibility of such damages.